REMARKS

Claims 2-24 are pending in this application. Applicants thank the Examiner for indicating the presence of allowable subject matter in claims 10-18.

Rejection Under 35 U.S.C. § 102

Claims 2-9 and 19-24 stand rejected under 35 § U.S.C. 102(e) as being anticipated by Vadekar U.S. Patent No. 7,020,281. Applicants respectfully traverse this rejection.

As set forth in MPEP § 2131, to anticipate a claim, the reference must teach every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The United States Court of Appeals for the Federal Circuit recently emphasized that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN v. Verisign*, No. 2007-1565, slip op. at 17-18 (Fed. Cir. Oct. 20, 2008) (emphasis added).

Applicants respectfully submit that the rejection fails to meet this requirement because the Office Action does not establish that Vadekar teaches every element of the claims arranged or combined in the same way as recited in the claims.

Exemplary embodiments encompassed by Applicants' claims are directed to cryptographic methods secured against a covert channel attack. In order to carry out a selected block of instructions as a function of an input variable amongst N predefined instruction blocks, a common block is carried out on the predefined N

instruction blocks, a predefined number of times, the predefined number being associated with the selected instruction block. The claimed subject matter can be advantageous for protecting algorithms during which a block of instructions from amongst several different blocks of instructions is executed as a function of an input variable. Such an algorithm can be, for example, a binary exponentiation algorithm performing a calculation of the type $B=A^D$, with A, B and D being integer numbers. Such an algorithm can be implemented in electronic devices, such as chip cards.

In known systems, an attack known as a timing attack can include measuring the time necessary for the device to execute a block of instructions between two test steps. If the execution times for the blocks of instructions Π_0, Π_1 (as shown in Applicants' Fig. 1) are different, then it is easy to identify a block of instructions Π_0 or Π_1 and to deduce therefrom the value of the associated input variable.

According to the claimed subject matter, a single elementary block (the common elementary block) can be effected regardless of the input variable. In other words, the common elementary block can be executed a predefined number of times according to the input variable. In contrast to known methods, different blocks of instructions are not executed as a function of the input variable. Thus, according to Applicants' claims, it is then not possible to determine, by means of a covert channel attack, which block of instructions is executed. Such a method according to the claims is therefore well protected in contrast to known methods.

Independent claim 21 recites a method for implementing a cryptographic calculation in an electronic device. The method can include selecting a block of instructions from amongst a plurality of predefined blocks of instructions, as a function of an input variable, and executing a set of instructions that is common to

the plurality of predefined blocks of instructions a predefined number of times. The predefined number is associated with the selected block of instructions.

Applicants respectfully submit that the same combination of elements is neither disclosed nor suggested by Vadekar. For example, the first cited section of Vadekar (col. 3, line 26 - col. 4, line 2) merely discusses known RSA and elliptic curve cryptography schemes, neither of which anticipates Applicants' claims.

The second cited section of Vadekar (col. 4, line 31 - col. 5, line 4) arguably discusses the desirability of preventing timing attacks by keeping the execution time and power identical for all possible execution paths through the loop. This section of Vadekar, however, discloses using a corrective subtraction when the loop terminates through the H0 path and similarly lacks the disclosure necessary to support the claimed "executing a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions."

Accordingly, Applicants respectfully submit that Vadekar fails to disclose every element of claim 21 arranged or combined in the same way as recited in the claim. Thus, claim 21 is allowable. This logic also disposes of the rejection of claims 2-9, 19-20 and 22-24, which depend directly or indirectly from claim 21.

Conclusion

For the foregoing reasons, Applicants respectfully submit that this application is in immediate condition for allowance and all pending claims are patentably distinct from the cited reference. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date December 24, 2008 By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839